CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being faxed to **571-273-8300** on the date shown below to **Mail Stop Appeal Brief - Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: June 6, 2011 Robin Wardzala
/Robin Wardzala/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Appellant(s):	David D. Brandt, *et al.*	Examiner:	Ronald Baum
Serial No:	10/661,696	Art Unit:	2439
Filing Date:	September 12, 2003		

Title: SYSTEM AND METHODOLOGY PROVIDING AUTOMATION SECURITY ANALYSIS, VALIDATION, AND LEARNING IN AN INDUSTRIAL CONTROLLER ENVIRONMENT

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Dear Sir:

Appellant submits this brief in response to an Examiner's Answer, dated April 5, 2011. It is believed that no payment is due. However, in the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 17-0026 [ALBRP303USC].

I. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 stand rejected and are under appeal.

II. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 are patentable under 35 U.S.C. §103(a) over Swiler, *et al.* (U.S. Patent 7,013,395 B1) in view of Townsend (U.S. Patent 6,374,358 B1), and further in view of Godwin (U.S. Patent Publication No. 2004/0059920 A1).

III. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 Under 35 U.S.C. §103(a)

Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Swiler, *et al.*, (U.S. 7,013,395 B1) in view of Townsend (U.S. 6,374,358 B1), and further in view of Godwin (U.S. 2004/0059920 A1).

1. Response to Examiner's Answer, Section 10(A-1)

In the Examiner's Answer, Section 10(A-1) (Response to Argument), it is alleged that Swiler, *et al.* discloses "a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication," as recited in Appellants' independent claim 1 (and similarly independent claims 12, 16, 17, and 30). Specifically, the Examiner notes that the analysis tool described in Swiler, *et al.* "[models] network risk via an attack graph (e.g., col. 4, lines 33-42) that is a function of at least the *attack templates and attacker profiles – both learned parameters used in the attack graph generation* – that are combined with (*i.e.* in the context of) the configuration file (e.g., col. 4, lines 43-58)" (emphasis added). However, although the Examiner ostensibly argues that such attack templates and attacker profiles read on the "learned pattern of communication" of independent claims 1, 12, 16, 17, and 30, it is again noted that these attack templates and attacker profiles are not obtained by *monitoring communication of data associated with an I/O table during a training period.* Rather, the attack templates and attacker profiles described in Swiler, *et al.* represent generic information about hypothetical attacker capabilities and attack steps (see at least column 4, lines 43-58 of Swiler, *et al.*). The cited reference does not indicate that such attack templates and attacker profiles are derived through monitoring of communication of data associated with an I/O table during a training period, and indeed the description of such attack templates and attacker profiles does not suggest that information gleaned through monitoring such data communication would be relevant in building such templates and profiles.

Moreover, information about *hypothetical attacker capabilities and attack steps*, as encoded in the indicated attack templates and attacker profiles, provides no data regarding a *learned pattern of communication.* Given that the indicated attack templates and attacker profiles of Swiler, *et al.* are not derived by *monitoring communication of data associated with an I/O table during a training period*, and do not represent a *learned pattern of communication*, the disclosure of such attack templates and attacker profiles in the cited reference would not lead one of ordinary skill to consider generating a learned pattern of communication by performing such monitoring.

Further regarding these aspects, the Examiner also indicates the configuration file described at column 5, line 55 – column 6, line 2 of Swiler, *et al.*, noting in particular that this configuration file "is a function of network topology detailed configurations of particular elements (e.g., col. 5, lines 55 – col. 6, line 2; IP addresses, port numbers/associated services)." The Examiner asserts that "the particular elements information had to have been monitored to be gathered to make the configuration file." However, it is noted that the information contained in the indicated configuration file – network configuration information, including IP addresses, machine types, operating systems, users, file system structures, etc. – do not represent *learned patterns of communication.* This is underscored by the fact that IP addresses, machine types, etc. represent *fixed* information that does not substantially change over time as a function of a detectable pattern. Furthermore, such information is not collected by *monitoring communication of data associated with an I/O table during a training period.* Rather, as indicated at column 5, lines 57-61 of Swiler, *et al.*, this configuration file information is merely read from machines on the network via polling. Since the information contained in the configuration files represent substantially fixed information, there is no motivation in Swiler, *et al.* to derive such information by monitoring the assets during a training period, much less by *monitoring communication of data associated with an I/O table during such a training period.*

In view of at least the above, as well as the arguments presented in Appellants' Appeal Brief, it is respectfully that Swiler, *et al.*, alone or in combination with the other references, fails to render obvious at least *a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication.*

2. Response to Examiner's Answer, Section 10(A-2)

In the Examiner's Answer, Section 10(A-2) (Response to Argument), it is alleged that Swiler, *et al.*, Townsend, and Godwin render obvious "an analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation," as recited in Appellants' independent claim 1 (and similarly independent claims 12, 16, 17, and 30). In particular, the Examiner repeats the assertion that Swiler, *et al.* discloses "a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication," as discussed above, and further argues that modifying Swiler, *et al.* using the Townsend's countermeasure aspects renders obvious the act of monitoring data traffic subsequent to a training period and generating a security output *if a current pattern of data traffic deviates from the learned pattern in excess of an acceptable deviation*.

However, Swiler, *et al.* does not *generate a learned pattern of communication* by any means, as noted supra, while Townsend merely generates security countermeasure recommendations based on information regarding the application assets and system architecture of an organization to be protected. Since neither Swiler, *et al.* nor Townsend contemplate, in general, a *learned pattern of communication*, it therefore follows that the cited references also fail to disclose or suggest *determining if a current pattern of data traffic deviates from such a learned pattern*, much less generating one or more security outputs if such a deviation occurs.

The Examiner also cites Godwin's tool for checking storage management security parameters, indicating in particular Godwin's automatic adjustment of security parameters. However, Godwin's parameter checks do not involve any manner of assessment on data traffic patterns generally. Instead, Godwin merely performs a check on each storage security parameter to ensure the parameter is within a compliant range pursuant to a security policy, rule, or allowable value. Like the other cited references, Godwin's tool makes no determination regarding whether *a current pattern of traffic data deviates from a learned pattern in excess of an acceptable deviation*, and thus does not remedy the shortcomings of the other cited reference in at least these regards.

See Appellants' Appeal Brief for additional arguments in connection with this rejection.

3. Response to Examiner's Answer, Section 10(A-3)

In the Examiner's Answer, Section 10(A-3) (Response to Argument), it is alleged that Swiler, *et al.*, Townsend, and Godwin render obvious "the analyzer component further performs an automated action that disables network requests from at least one outside network upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation," as recited in Appellants' claim 49. Without conceding the propriety of the remarks in the Examiner's Answer, Appellant has no further arguments with respect to claim 49.

Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 17-0026 [ALBRP303USC].

Respectfully submitted,

Dated: June 6, 2011

By: /Brian Steed/
Brian Steed, Reg. No. 64,095

TUROCY & WATSON, LLP
127 Public Square
57th Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731

IV. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A security analysis tool for an automation system having a controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the security analysis tool comprising:

a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication; and

an analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation, the one or more security outputs including at least one output that alters the data traffic between the controller and the at least one I/O device.

2. The tool of claim 1, further comprising an interface component that generates a description of one or more industrial controllers in the automation system.

3. The tool of claim 2, wherein at least one of the interface component or the analyzer component operate on a computer and receive one or more factory inputs that provide the description, the factory inputs include at least one of user input, model inputs, schemas, formulas, equations, files, maps, or codes.

4. The tool of claim 3, wherein the factory inputs are processed by the analyzer component to generate the security outputs, the security outputs including at least one of manuals, documents, schemas, executables, codes, files, e-mails, recommendations, topologies, configurations, application procedures, parameters, policies, rules, user procedures, or user practices that are employed to facilitate security measures in an automation system.

5. The tool of claim 2, wherein the interface component includes at least one of a display output having associated display objects and at least one input to facilitate operations with the analyzer component, the interface component is associated with at least one of an engine, an application, an editor tool, a web browser, or a web service.

6. The tool of claim 5, wherein the display objects include at least one of configurable icons, buttons, sliders, input boxes, selection options, menus, or tabs, the display objects having multiple configurable dimensions, shapes, colors, text, data and sounds to facilitate operations with the analyzer component.

7. The tool of claim 5, the at least one input includes user commands from at least one of a mouse, a keyboard, speech input, a web site, a remote web service, a camera, or video input to affect operations of the interface component and the analyzer component.

8. The tool of claim 2, wherein the description includes a model of one or more industrial automation assets to be protected and associated network pathways to access the one or more industrial automation assets.

9. The tool of claim 2, wherein the description includes at least one of risk data or cost data that is employed by the analyzer component to determine suitable security measures.

10-11. (Cancelled)

12. A security analysis method for use in an industrial automation system having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the method comprising:

monitoring communication of data associated with the I/O table for a predetermined training period to learn at least one learned pattern of communication;

defining a pattern threshold specifying an acceptable deviation from the at least one learned pattern;

monitoring data traffic subsequent to the training period; and

performing at least one automated security event if a current pattern of the data traffic deviates from the at least one learned pattern in excess of the acceptable deviation after the training period,

wherein performing the at least one automated security event includes at least altering a network traffic pattern between the industrial controller and the I/O device.

13. The method of claim 12, further comprising:

inputting at least one model related to one or more industrial controllers;

generating one or more security outputs based on the at least one model; and automatically installing one or more security components based at least in part on the one or more security outputs.

14. The method of claim 13, wherein generating the one or more security outputs includes generating one or more security outputs that include at least one of recommended security components, codes, parameters, settings, related interconnection topologies, connection configurations, application procedures, security policies, rules, user procedures, or user practices.

15. The method of claim 13, further comprising:

automatically deploying the one or more security outputs to the industrial controller; and

utilizing the one or more security outputs to mitigate at least one of unauthorized network access or network attack.

16. A security analysis system in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, comprising:

means for monitoring communication of data associated with the I/O table for a predetermined training period;

means for learning at least one learned pattern of communication based on the means for monitoring;

means for defining a pattern threshold that specifies an acceptable deviation from the learned pattern;

means for automatically detecting that a current pattern of communication of the data associated with the I/O table deviates from the learned pattern in excess of the acceptable deviation after the training period; and

means for performing an automated action that alters the current pattern of communication in response to the detecting.

17. A security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the system comprising:

a learning component that monitors communication of data associated with the I/O table with respect to the industrial controller during a training period and establishes a learned pattern of communication; and

an analyzer component that monitors a current pattern of communication of the data associated with the I/O table subsequent to the training period and automatically performs a security action to bring the current pattern in line with the learned pattern in response to detecting that the current pattern communication has deviated from the learned pattern of access in excess of a defined pattern threshold.

18. (Cancelled)

19. The system of claim 17, further comprising:

a scanner component that automatically interrogates at least one of the industrial controller, the I/O device, or the controlled device at periodic intervals for security-related data;

a validation component that automatically assesses security capabilities of the at least one of the industrial controller, the I/O device, or the controlled device based upon a comparison of the security-related data and one or more predetermined security guidelines; and

a security analysis tool that recommends at least one network interconnection to achieve a specified security goal indicated by the predetermined security guidelines.

20. The system of claim 19, wherein the security guidelines are automatically determined.

21. The system of claim 46, wherein the host-based component performs vulnerability scanning and auditing on devices, and the network-based component performs vulnerability scanning and auditing on networks.

22. (Cancelled)

23. The system of claim 21, wherein at least one of the host-based component or the network-based component at least one of non-destructively maps a topology of information technology (IT) and industrial automation devices, checks revisions and configurations, checks user attributes, or checks access control lists.

24. (Cancelled)

25. The system of claim 17, wherein the security action includes at least one of automatically correcting the security events, automatically adjusting security parameters, altering network traffic patterns, adding security components, removing security components, triggering alarms, automatically notifying entities about detected problems and concerns, generating an error or log file, generating a schema, generating data to re-configure or re-route network connections, updating a database, or updating a remote site.

26-29. (Cancelled)

30. (Currently Amended) An automated security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, comprising:

means for monitoring communication of data associated with the I/O table with respect to the industrial controller during a training period and establishing a learned pattern of communication;

means for defining a pattern threshold specifying an allowable deviation from the learned pattern;

means for monitoring a current pattern of communication of the data associated with the I/O table subsequent to the training period; and

means for initiating a security procedure that performs a security action to bring the current pattern in line with the learned pattern if the means for monitoring identifies that a current access pattern deviates from the at least learned pattern in excess of the allowable deviation.

31-40. (Cancelled)

41. The tool of claim 1, further comprising a validation component that periodically monitors the controller following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto.

42-44. (Cancelled)

45. The tool of claim 1, the analyzer component is adapted for partitioned security specification entry and sign-off from various groups.

46. The system of claim 19, the scanner component and the validation component are at least one of a host-based component or a network-based component.

47. The system of claim 21, at least one of the host-based component or the network-based component at least one of determines susceptibility to common network-based attacks, searches for open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports, scans for vulnerable network services, attempts to gain identity information about end devices that relates to hacker entry, or performs vulnerability scanning and auditing on firewalls, routers, security devices, and factory protocols.

48. The system of claim 41, the validation component automatically installs one or more security components in response to the one or more vulnerabilities.

49. The system of claim 1, wherein the analyzer component further performs an automated action that disables network requests from at least one outside network upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation.

50. The system of claim 12, wherein the at least one automated security event includes at least disabling network attempts to access the industrial controller.

51. The method of claim 12, wherein the monitoring communication of data comprises at least one of monitoring a number of network requests to or from the industrial controller over a given time frame or monitoring a type of request to or from the industrial controller during the training period.

52. The tool of claim 1, wherein the one or more security outputs alter the data traffic between the controller and the at least one I/O device to restore the learned pattern.

V. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

VI. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.